

RECEIVED

2019R00047/APT/DEM

JAN 29 2020

AT 8:30 ^V M
WILLIAM T. WALSH, CLERK

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

FILED

JAN 28 2020

AT 8:30 ⁴³⁰ PM
WILLIAM T. WALSH, CLERK ^{JB}

UNITED STATES OF AMERICA : Hon.
 :
 v. : Crim. No. 20- 97 (FLW)
 :
 MOHSIN RAZA, : 18 U.S.C. §§ 1028(f), 1028(a)(2),
 a/k/a "Mohsin Raza Amiri," and : 1543, 1028A, and 2
 MUJTABA ALI RAZA, :
 a/k/a "Mujtaba Ali Lilani," :
 a/k/a "Mujtaba Ali," :
 a/k/a "Mujtaba" :

INDICTMENT

The Grand Jury in and for the District of New Jersey, sitting in Newark,
charges:

COUNT ONE

(Conspiracy to Produce and Transfer False Identification Documents)

1. At all times relevant to this Indictment:

Individuals and Entities

a. Defendants MOHSIN RAZA, a/k/a "Mohsin Raza Amiri," and
MUJTABA ALI RAZA, a/k/a "Mujtaba Ali Lilani," a/k/a "Mujtaba Ali," a/k/a
"Mujtaba," resided in or around Karachi, Pakistan.

b. Defendants MOHSIN RAZA and MUJTABA ALI RAZA, together
with others known and unknown to the Grand Jury, operated a fraudulent online
business, based in or around Karachi, Pakistan, named, at various times,
"SecondEye Solution" and "Forwarderz" (collectively, "SecondEye"). SecondEye,
through its website, electronically produced, sold, and transferred digital versions
of (i) false identity documents, including passports, driver's licenses, national
identity cards, and social security cards associated with more than two hundred

countries and territories, including the United States (“False Identification Documents”); and (ii) invoices, credit card statements, business licenses, and bank statements (“False Business Records”) (collectively, “False SecondEye Documents”). SecondEye operated on a global scale, selling and transferring False SecondEye Documents to individuals throughout the world, including in New Jersey.

c. “Company-1” was a financial technology company headquartered in or around San Jose, California.

d. “Company-2” was an e-commerce and cloud computing company headquartered in or around Seattle, Washington.

e. “Company-3” was a social media and social networking service headquartered in or around Menlo Park, California.

f. “Company-4” was an e-commerce and international money transfer business headquartered in or around London, United Kingdom.

g. “Company-5” was an online money transfer and digital payment services company headquartered in or around New York, New York.

h. “Company-6” was an international money transfer business and virtual currency exchange registered in Panama and headquartered in Switzerland and Hong Kong.

i. “Company-7” was a virtual currency exchange headquartered in or around Seattle, Washington.

j. “Company-8” was a file hosting company headquartered in or around San Francisco, California.

k. “Company-9” was a file hosting company headquartered in or around Auckland, New Zealand.

l. “Financial Institution-1” was a commercial banking and financial services company headquartered in or around Karachi, Pakistan.

The Conspiracy

2. From at least as early as 2011, through on or about the date of this Indictment, in the District of New Jersey, and elsewhere, the defendants,

MOHSIN RAZA,
a/k/a “Mohsin Raza Amiri,” and
MUJTABA ALI RAZA,
a/k/a “Mujtaba Ali Lilani,”
a/k/a “Mujtaba Ali,”
a/k/a “Mujtaba,”

did knowingly and intentionally conspire and agree with each other and others:

a. to knowingly and without lawful authority produce identification documents, authentication features, and false identification documents, to wit, False Identification Documents, the production of which was in and affected interstate and foreign commerce, and the offense involved the production of identification documents, authentication features, and false identification documents that appeared to be (i) identification documents and authentication features issued by and under the authority of the United States; and (ii) driver’s licenses and personal identification cards, and the offense involved

the production of more than five identification documents, authentication features, and false identification documents, contrary to Title 18, United States Code, Sections 1028(a)(1), (b)(1)(A) & (B), & (c)(3)(A); and

b. to knowingly transfer identification documents, authentication features, and false identification documents, knowing that such documents and features were produced without lawful authority, to wit, False Identification Documents, the transfer of which was in and affected interstate and foreign commerce, and the offense involved the transfer of identification documents, authentication features, and false identification documents that appeared to be (i) identification documents and authentication features issued by and under the authority of the United States; and (ii) driver's licenses and personal identification cards, and the offense involved the transfer of more than five identification documents, authentication features, and false identification documents, contrary to Title 18, United States Code, Sections 1028(a)(2), (b)(1)(A) & (B), & (c)(3)(A).

Goal of the Conspiracy

3. The goal of the conspiracy was for MOHSIN RAZA, MUJTABA ALI RAZA, and their co-conspirators to enrich themselves by producing, selling, and transferring False Identification Documents through SecondEye.

Manner and Means of the Conspiracy

4. It was part of the conspiracy that:

a. The defendants and their co-conspirators, through SecondEye, provided customers electronic images of False SecondEye Documents, but not the physical documents themselves. The False SecondEye Documents were the type commonly needed and used to create online accounts at banks, payment processors, social media sites, and digital currency platforms.

b. SecondEye offered hundreds of types of False SecondEye Documents for sale through its website, which provided, for example, that a passport could be purchased for \$30, a driver's license for \$30, and a "selfie" photograph of an individual holding a False SecondEye Document for \$50. For documents that required a photograph of the document holder, SecondEye provided its customers with the option of either supplying a photograph or using a photograph supplied by SecondEye.

c. The defendants and their co-conspirators advertised SecondEye's services online on at least one well-known cyber hacker forum (the "Forum"). SecondEye advertised that the False SecondEye Documents could be used by its customers to prove identity as needed to access and use online accounts at payment processors, social media sites, and digital currency platforms. SecondEye further advertised that the False SecondEye Documents could be used by customers who were "banned" or "suspended" to restore access to their online accounts.

d. The defendants and their co-conspirators communicated directly with SecondEye customers through email and the Forum as well as through various chat platforms. For example:

i. On July 3, 2014, MUJTABA ALI RAZA communicated with a SecondEye customer through the Forum. The customer stated, in part, "I'd like to purchase a vcc [virtual credit card] to verify my [Company-1], it's a USA [Company-1], which now is requiring my SSN [social security number] which I won't provide to them, but i just want a VCC to raise the limit of withdrawing funds, my question is, i got a limit of \$500, how much will it be raised after being verified with VCC?" MUJTABA ALI RAZA responded, "It will be increased but dont know how much it will be increased" and signed the email "Secondeye."

ii. On or about December 12, 2018, a SecondEye customer emailed a SecondEye email account and stated, "I am trying to register a [Company-1] account and see if they accept all my fake docs before i try to use it. You say you help with a SSN Document. How would that work if they ask for it?" A co-conspirator responded, "we can make ssn [social security number] document which number you provide us and we do not provide guarantee for any documents but our customers did many times by using our documents, what we provide is just a original looking documents."

iii. On or about December 24, 2018, a co-conspirator, using a SecondEye email address, sent an email to a SecondEye customer. The email,

signed “SecondEye (Customer Care 3),” advised, “we can only provide ssn document (not ssn number) we can make ssn document which [sic] number you provide us.” The customer then asked, “[d]o you happen to know whether I’d be able to get a SSN from somewhere to submit it to [Company-1]?” A co-conspirator replied, “you can find on net some one who provide real ssn number.”

e. The defendants and their co-conspirators communicated with each other through email regarding the operation of SecondEye. For example:

i. On or about January 7, 2015, MOHSIN RAZA sent an email to MUJTABA ALI RAZA, who was using an email address associated with SecondEye, providing information about the payment of salary for MUJTABA ALI RAZA.

ii. On at least three occasions between on or about July 27, 2017 and on or about September 27, 2018, MUJTABA ALI RAZA sent emails to MOHSIN RAZA, which included login passwords for various third-party payment accounts that SecondEye used to accept funds from SecondEye customers, as well as email accounts, social media accounts, and accounts at web hosting companies that were used to operate and promote SecondEye.

iii. On or about October 8, 2018, a co-conspirator sent an email to MOHSIN RAZA listing salaries for nine SecondEye employees.

f. The defendants and their co-conspirators posted advice for SecondEye customers on the SecondEye website about how to use the False

SecondEye Documents. For example, on a date prior to on or around January 16, 2017, a co-conspirator posted a link on the SecondEye website titled "I am Scared of uploading Fake CC [credit card] Statement to [Company-1] – What will happen next?" Upon clicking the link, the following text appeared:

Problem:

[Company-1] is asking me to upload Credit Card statement. I need to know that what if I provide fake Credit Card statement to [Company-1], will they permanent ban my account if they know it or what

Solution:

Your [Company-1] account is already limited and you have no other option to restore it except to provide a Credit Card statement. If you had added a real card then still there is no guarantee that they will restore your account after providing your real Credit Card statement. if they get suspicious regarding your transactions or account activity they will simply close your account by mentioning high risk activity or other.

If your account is stealth and required a Credit Card statement to restore it then you need to place an order for a Fake Credit Card statement. As per our experience we had restored many accounts but still there is not guarantee of restoration. You can try your luck.

We had also restored [Company-1] accounts that demands for Bank statement, Photo ID, Proof of Address, Business Details and other.

To order a Credit Card statement from us, we just need your Credit Card details that you had provided to [Company-1] and other transaction details like withdrawal or upload history or [Company-1] code to confirm owner of card if you have.

Credit Card statement available for all Visa Card, Master Card, Gift and Prepaid cards as per your request.

Please Visit our website to place your order.

g. The defendants and their co-conspirators accepted funds from SecondEye customers that were denominated in fiat currencies through online payment processors, international money transfer businesses, and other international financial institutions, including Company-1, Company-4, Company-5, Company-6, and Financial Institution-1.

h. The defendants and their co-conspirators also accepted funds from SecondEye customers in the form of virtual currencies, including Bitcoin, through various virtual currency exchanges, including Company-7. During the relevant time-period, defendants and their co-conspirators accepted in excess of \$1.5 million in Bitcoin transfers alone from SecondEye customers related to the purchase of the False SecondEye Documents. Those funds were received in more than 20,000 separate transactions.

i. The defendants and their co-conspirators transferred thousands of False SecondEye Documents to SecondEye customers through various electronic means, including email and file hosting services located in the United States and abroad. For example:

i. On or about December 17, 2017, via electronic means, a co-conspirator transferred the image of a false Illinois driver's license, bearing the name of real U.S. person, to a SecondEye customer.

ii. On or about March 5, 2019, via a file hosting account at Company-8, a co-conspirator transferred a false New Jersey Driver's License, a photograph of an individual holding the same New Jersey Driver's License, and a U.S. Passport, all bearing the name of an individual with initials M.M., to a recipient located in New Jersey.

iii. On or about July 31, 2019, via a file hosting account at Company-9, a co-conspirator transferred a false New Jersey Driver's License, bearing the name of an individual with initials M.E., to a recipient located in New Jersey.

iv. On or about January 12, 2020, via a file hosting account at Company-8, a co-conspirator sent a false non-immigrant visa, bearing the name of an individual with initials C.A., to a recipient located in New Jersey.

j. Between in or around September 2013 through in or around June 2019, MOHSIN RAZA controlled a bank account at Financial Institution-1, which he used to transfer funds to employees of SecondEye.

k. Customers of SecondEye used the False SecondEye Documents to commit and facilitate the commission of various cybercrimes and other criminal conduct. For example:

i. On or about December 13, 2017, a SecondEye customer ("Customer-1") purchased a false Illinois driver's license in the name of a real U.S. person. Customer-1 told SecondEye that the license would be used for "verification

for some online purchase.” After receiving the license, Customer-1 and others used the false license and identity to obtain information about hundreds of users of a virtual currency exchange platform as part of a scheme to steal the users’ virtual currency. Customer-1 and others thereafter stole at least \$1.4 million in virtual currency using the false license.

ii. Between on or about May 11, 2017 through on or about September 16, 2017, at least one member of the Internet Research Agency LLC (the “Organization”), a Russian organization that interfered with elections and political processes, including the 2016 U.S. presidential election, purchased multiple false identification documents from SecondEye in the names of real U.S. persons and fictitious persons. Thereafter, the false identification documents were used as supporting documents for accounts previously opened by the Organization at Company-3 in support of the Organization’s operations.

iii. SecondEye customers used the False SecondEye Documents to defraud payment processing companies, including Company-1; e-commerce businesses, including Company-2; social media and social networking platforms, including Company-3; and virtual currency exchanges, both foreign and domestic, by gaining unauthorized access to online platforms provided by such entities, often to gain access to customer accounts that previously had been revoked or suspended.

All in violation of Title 18, United States Code, Section 1028(f).

COUNTS TWO THROUGH FOUR

(Transferring False Identity Documents)

1. The allegations set forth in Paragraph 1 and Paragraphs 3 through 4 of Count One of this Indictment are re-alleged and incorporated as if fully set forth herein.

2. On or about the dates set forth in the table below, in the District of New Jersey, and elsewhere, the defendants,

MOHSIN RAZA,
a/k/a "Mohsin Raza Amiri," and
MUJTABA RAZA,
a/k/a "Mujtaba Ali Lilani,"
a/k/a "Mujtaba Ali,"
a/k/a "Mujtaba,"

did knowingly transfer an identification document, authentication feature, and a false identification document, knowing that such document and feature was produced without lawful authority, the transfer of which was in and affected interstate and foreign commerce, to wit, each False Identification Document described in the table below, which, as specified below, appeared to be (i) an identification document and authentication feature issued by and under the authority of the United States; and (ii) a driver's license and personal identification card, each constituting a separate count of this Indictment:

<u>Count</u>	<u>Approx. Date</u>	<u>False Identification Document Description</u>	<u>Initials</u>	<u>Statutory Subsection</u>
2	3/5/19	New Jersey Driver's License and U.S. Passport	M.M.	18 U.S.C. § 1028(b)(1)(A)(i) & (ii)

3	7/31/19	New Jersey Driver's License	M.E.	18 U.S.C. § 1028(b)(1)(A)(ii)
4	1/12/20	Non-Immigrant Visa for a Foreign Passport	C.A.	18 U.S.C. § 1028(b)(1)(A)(i)

In violation of Title 18, United States Code, Sections 1028(a)(2), (b)(1)(A), & (c)(3)(A), and 2.

COUNT FIVE
(False Use of a Passport)

1. The allegations set forth in Paragraph 1 and Paragraphs 3 through 4 of Count One of this Indictment are re-alleged and incorporated as if fully set forth herein.

2. On or about March 5, 2019, in the District of New Jersey, and elsewhere, the defendants,

MOHSIN RAZA,
a/k/a "Mohsin Raza Amiri," and
MUJTABA RAZA,
a/k/a "Mujtaba Ali Lilani,"
a/k/a "Mujtaba Ali,"
a/k/a "Mujtaba,"

did willfully and knowingly use, attempt to use, and furnish to another for use, a false, forged, and counterfeited passport and instrument purporting to be a passport issued under the authority of the United States.

In violation of Title 18, United States Code, Sections 1543 and 2.

COUNT SIX
(Aggravated Identity Theft)

1. The allegations set forth in Count One of this Indictment are re-alleged and incorporated as if fully set forth herein.

2. From at least as early as 2011, through on or about the date of this Indictment, in the District of New Jersey, and elsewhere, the defendants,

MOHSIN RAZA,
a/k/a "Mohsin Raza Amiri," and
MUJTABA RAZA,
a/k/a "Mujtaba Ali Lilani,"
a/k/a "Mujtaba Ali,"
a/k/a "Mujtaba,"

knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person, namely, the name and date of birth of G.B., during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), to wit, the conspiracy to produce, and transfer, false identification documents, in violation of Title 18, United States Code, Section 1028(f), set forth in Count One of this Indictment, knowing that the means of identification belonged to another actual person.

In violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

FORFEITURE ALLEGATION AS TO COUNTS ONE THROUGH FOUR

1. As a result of committing the offenses in violation of 18 U.S.C. § 1028 alleged in Counts One through Four of this Indictment, the defendants, MOHSIN RAZA and MUJTABA ALI RAZA, shall forfeit to the United States:

- (a) pursuant to 18 U.S.C. § 982(a)(2)(B), any property constituting, or derived from, proceeds obtained directly or indirectly, as a result of such offenses; and
- (b) pursuant to 18 U.S.C. § 1028(h), any and all illicit authentication features, identification documents, document-making implements and means of identification;

FORFEITURE ALLEGATION AS TO COUNT FIVE


2. As a result of committing the use of false passports offense charged in Count Five of this Indictment, the defendants, MOHSIN RAZA and MUJTABA ALI RAZA, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 1594(d), any property, real or personal, constituting or derived from any proceeds the defendant obtained, directly or indirectly, as a result of the offense, and any property, real or personal, involved in, used, or intended to be used to commit or to facilitate the commission of the offense alleged in Count Five of this Indictment, and any property traceable to such property.

SUBSTITUTE ASSETS PROVISION

3. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

- (a) cannot be located upon the exercise of due diligence;
- (b) has been transferred or sold to, or deposited with, a third person;
- (c) has been placed beyond the jurisdiction of the Court;
- (d) has been substantially diminished in value; or
- (e) has been commingled with other property which cannot be subdivided without difficulty;

it is the intent of the United States, pursuant to 21 U.S.C. § 853(p), as incorporated by 28 U.S.C. § 2461(c), to seek forfeiture of any other property of the defendant up to the value of the above-described forfeitable property.



CRAIG CARPENITO
United States Attorney

CASE NUMBER: 20-cv-97-FLW

**United States District Court
District of New Jersey**

UNITED STATES OF AMERICA

v.

**MOHSIN RAZA,
a/k/a "Mohsin Raza Amiri," and
MUJTABA ALI RAZA
a/k/a "Mujtaba Ali Lilani"
a/k/a "Mujtaba Ali"
a/k/a "Mujtaba"**

INDICTMENT FOR

**18 U.S.C. § 1028(f)
18 U.S.C. § 1028(a)(2)
18 U.S.C. § 1543
18 U.S.C. § 1028A
18 U.S.C. § 2**

CRAIG CARPENTO
UNITED STATES ATTORNEY
NEWARK, NEW JERSEY

ANTHONY P. TORNTORE
DAVID E. MALAGOLD
ASSISTANT U.S. ATTORNEYS
973-645-2726
973-645-6103